DD/S 64-1331

SECRET

DD/S REGISTRY
FILE Security 5

5 MAR 1964

MEMORANDUM FOR: D/DCI/NIPE

25X1 ATTENTION : [redacted]

THROUGH : Deputy Director for Support

SUBJECT : Office of Security Reactions to Recommendations No. 4, No. 6, No. 8, No. 9, No. 10, No. 12, No. 13 and No. 21 of FIAB Report Inspired by the Dunlap Case.

REFERENCE : Memorandum to Chairman, USIB from Mr. McGeorge Bundy, Dated 8 February 1964; Subject: Measures for Strengthening the Counterintelligence Posture of the United States.

1. This memorandum is for your information and contains Office of Security suggestions regarding eight of the Recommendations contained in referenced document.

2. It is understood here that the CI Staff will be responsible for the preparation of the suggested response by the DCI to Recommendation No. 11. It is further understood that the DDP, in coordination with appropriate elements of the State Department, will prepare coordinated responses to Recommendations No. 14, No. 15, No. 16 and No. 17. Finally, it should be noted that the necessary coordination regarding Recommendation No. 7 is currently underway and the Department of Defense will prepare a response on this Recommendation only after coordination with the Agency, specifically the Office of Security.

Recommendation No. 4: That, within each sensitive agency where the practice is not now being followed: (a) strict personnel security standards, including standards of personal conduct, be applied to all

SECRET

personnel having access to sensitive information or sensitive operations; (b) that these standards be applied equally to civilian and military personnel regardless of rank; and (c) that serious questions of doubt concerning personnel having such access be resolved in favor of the national security.

Concur. It should be the goal of the intelligence community to establish standardized and strict personnel security criteria for all personnel, military and civilian, participating in intelligence activities. All personnel having access to sensitive information or sensitive operations should meet like security criteria prior to access and their continued security well-being should be monitored thereafter on a generally uniform basis.

A standardized security program for all intelligence personnel could best be achieved by each agency developing centralized security control from an organizational standpoint together with uniform criteria and standardized techniques for the application of the criteria. Such standardized security programs would greatly facilitate the exchange of personnel between departments and agencies and would enhance greater participation in joint projects without security variations.

A standardized security program for intelligence personnel would lead to a more uniform approach to the resolution of questions involving an individual's suitability and would certainly foster the protection of national security interests.

The Security Committee of the USIB could assist in the development of uniform personnel security standards and the preparation of guidelines for the monitoring of personal conduct.

Recommendation No. 6: That, as a means of achieving major counterintelligence objectives, actions be taken within the sensitive agencies, as required, to assure the conduct of periodic, comprehensive, inspections concerning the adequacy of compliance with approved policies relating to personnel security investigations and clearances, security suspension of employees, physical security, document control, and the like.

Concur. An inherent part of an effective security program is a system of periodic inspections to ensure the adequacy of all aspects of security. Such inspections are best conducted by an independent authority such as the inspector-general facility. In addition, security officers themselves should continuously study and seek improvement in the programs they implement and administer.

Since the USIB Policy Statement on Counterintelligence and Security Responsibilities (USIB-D-1.5/24 Approved 18 July 1962) calls for semi-annual reports on security and counterintelligence developments in the agencies, inspection-inspired changes could be included in these same reports. The Guide on Security and Counterintelligence Practices and Procedures to the Policy Statement sets forth the essentials of a basic security program, and utilization of this Guide as an aid to security surveys would be beneficial. The Security Committee, USIB, will, if called upon, assist in the development of additional formats.

> Recommendation No. 8: That arrangements be made within each sensitive agency, as required, to assure that security counterintelligence-oriented personnel participate in the timely review at the Headquarters level of all questionable personnel security cases which develop within that agency.

Concur. Each agency or department should have a system providing for security-counterintelligence reviews of questionable personnel security cases. Such security cases should be reviewed and closely monitored by security personnel with the highest degree of understanding and sophistication in opposition penetration techniques. All investigative assets and capabilities should be utilized to the fullest extent in such cases.

> Recommendation No. 9: That, in the continuing effort to instill an enhanced sense of security responsibility on the part of all personnel in the sensitive agencies, the Dunlap case be used in the security indoctrination processes of those agencies as a striking example of a most serious espionage penetration and of the failure to inculcate the degree of security consciousness which should obtain among the personnel of all sensitive agencies.

Concur. The Dunlap, Scarbeck and similar cases, properly presented, can be used effectively by security education officers throughout the intelligence community to enlighten personnel on the subversive efforts of the opposition. Actual cases serve to illustrate clearly and dramatically the techniques and approaches utilized. There are definite advantages to the preparation of standardized write-ups for the use of various agencies and these could be prepared by the Security Committee of USIB.

> Recommendation No. 10: That investigative and security-review personnel associated with sensitive activities be provided with more sophisticated and professional information and guidance concerning the nature and potential security implications of abnormal sexual activities, such as homosexuality and perversion, which they encounter in the course of their inquiries and interviews.

Concur. Security review personnel must operate on the highest level of sophistication in such matters as the adjudication of security cases involving abnormal sexual problems. Such professionalism can be enhanced by the exchange of approved definitions and criteria. There is information and material within the community which is suitable for distribution. Exchanges can probably best be accomplished through controlled security channels such as the Security Committee of USIB and such exchanges should be made.

> Recommendation No. 12: That, apart from any action taken on the preceding recommendation concerning the establishment of a counterintelligence mechanism, immediate action be taken to assure that any agency having action responsibility in a personnel-security type case is promptly furnished all pertinent information possessed by other departments and agencies.

Concur. The rapid exchange of security information on critical cases is of the highest order of importance. Effective action depends upon collation and evaluation of all pertinent information and these activities should be conducted as expeditiously as possible. The agency having action responsibility should promptly make known its need for information to all agencies which could be of help. All agencies so notified should ensure that the responsible agency is furnished pertinent information on an expedite basis and should offer all possible assistance.

Recommendation No. 13: That the National Security Agency, and other sensitive agencies as appropriate, take steps to assure that the "need-to-know" principle is applied rigorously in the granting of access to sensitive information.

Concur. Access to sensitive information is, for the most part, highly controlled and maintained through established systems of compartmentation; for example, the systems established for T-KH and communications intelligence. The number of clearances for access to such information is intended to be carefully controlled and the granting of a clearance should only follow a clearly justified "need-to-know." This general philosophy is followed within each of the agencies and departments within the intelligence community.

The degree of access of an individual once cleared is a problem for each component and office within the community to consider and resolve. The strict enforcement of the "need-to-know" principle within this framework is difficult to assure absolutely. However, each of the components and offices is aware of the requirements of the "need-to-know" principle and it should not be necessary for the principle to be reaffirmed anew periodically since it is already the most basic tenet of security within the intelligence community.

The complex nature of systems of compartmentation governing access to sensitive information does not lend easy solutions to problems which are inherent in the management and operation of the systems. The management of the T-KH system is currently under study by CIA and the broad problem of sanitization and downgrading of sensitive intelligence is currently under study by the Security and COMOR Committees. The results of such studies will be available to all agencies of the community.

The Security Committee of USIB can serve to disseminate any data, information and results of studies as well as continuing to serve as a forum in the discussion of such problems.

Recommendation No. 21: That the White House be informed promptly of developing situations indicating the likelihood of the existence of a serious penetration of any sensitive activity of our Government.

Concur. The USIB department or agency having primary responsibility in a case involving possible penetration should notify the Special Assistant

to the President for National Security Affairs and the USIB. Notification should be made in those cases which have developed to the point where a serious penetration of a U. S. intelligence activity is indicated.

3. This Office is prepared to provide you with any additional assistance you may seek in the packaging of the final response to Mr. Bundy due by 10 March.

SIGNED

R. L. Bannerman
Director of Security

Distribution:
Orig. & 2 - Adse.
1 - DDS SUBJECT

☐ UNCLASSIFIED ☐ INTERNAL USE ONLY ☐ CONFIDENTIAL ☒ SECRET

ROUTING AND RECORD SHEET

SUBJECT: (Optional) Office of Security Reactions to Recommendations #4, #6, #8, #9, #10, #12, #13 and #21 of FIAB Report Inspired by the Dunlap Case.

FROM: Director of Security
4-E-60

NO.

DATE 5 MAR 1964

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
1. DDS Rm. 7-D-18		3-6-61	/s/ LKW	To: #1
2. D/DCI/NIPE [redacted] Rm. 7-E-22				After the Office of Security received the Top Secret document from McGeorge Bundy on the Subject, "Measures for Strengthening the Counterintelligence Posture of the United States" (which was sent to your office earlier under separate cover for security control reasons), a meeting was held with representatives of the DDP and John Bross' office. At that time it was decided that the Office of Security should respond directly to 8 of the recommendations and that this office should have coordinating concerns with certain of the others as explained in the attached. Responsibility for pulling together the total package for the DCI's signature rests with [redacted] per agreement reached at the meeting.
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

25X1

25X

/s/
R. L. Bannerman

FORM 1 USE 610 [illegible] ☐ SECRET ☐ CONFIDENTIAL ☐ USE ONLY ☐ UNCLASSIFIED